

ŠPECIFIKÁCIA PREDMETU ZMLUVY

Predmetom zákazky je celkové zvýšenie bezpečnosti IT infraštruktúry, ktoré je nevyhnutné k splneniu legislatívnych požiadaviek, t.j. bezpečnostných štandardov a znalostných štandardov v oblasti kybernetickej bezpečnosti, stanovených všeobecne záväzným právnym predpisom Národného bezpečnostného úradu podľa § 32 ods. 1 písm. d) zákona č. 69/2018 Z.z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov. Predmetom zákazky je aplikácia súboru riešení, ktoré boli navrhnuté na základe zistení nedostatkov z auditu kybernetickej bezpečnosti a potreba realizácie nevyhnutných krokov na ich odstránenie. Zákazka sa skladá z dvoch celkov, ktoré spolu súvisia a spolu tvoria opatrenia, ktoré posilnia odolnosť proti kybernetickým útokom. Po povýšení doménových radičov a implementácii bezpečnostných opatrení sa okrem zvýšenia bezpečnosti očakáva aj väčšia stabilita vybraných systémov, Poskytovanie podpory sa požaduje na obdobie 36 mesiacov. Všetky dodané licencie musia byť nové, doposiaľ nepoužívané.

Celok A): Povýšenie Doménových radičov, upgrade adresárovej služby (Active Directory (ďalej aj „AD“))

Predmetom zákazky v celku A) je povýšenie OS doménových radičov (Domain Controller (ďalej aj „DC“)) z aktuálnej verzie Windows server 2012 na Windows server 2022. Tieto servery slúžia pre správu domény BVSNET, ktorá je primárnou doménou obstarávateľa a je využívaná v rámci centralizovanej správy a riadenia zdrojov, či už sa jedná o sieťové zdroje alebo o autorizáciu užívateľov.

1. Dodávka licencií

Špecifikácia	Zoznam potrebných licencií	Počet
Licencia USER CALL	Windows Server - User CAL 2022	700 ks
Licencia Data Center	Windows Server Datacenter per Core 16 SW License 2022	8 ks

2. Inštalčné, implementačné práce a migrácia

Popis	Jednotka	Počet
Analýza	súbor	1
<p>Pred migračná analýza aktuálneho stavu DC (tri doménové radiče). Obstarávateľ má aktívnych 1200 užívateľských účtov (Obstarávateľ v súčasnosti vlastní 500 ks User CAL 2022).</p> <p>Obstarávateľ taktiež spravuje 700 koncových zariadení a 150 serverov zaradených do domény.</p> <p>Analýza možnosti zvýšenia Forest and Domain Functional Levels.</p>		
Migrácia	súbor	1
Migrácia DC z aktuálnej verzie Windows server 2012 na Windows server 2022.		
Testovanie	súbor	1
<p>Testovanie fail-over clustra AD.</p> <p>Testovanie AD serverov a kontrola synchronizácie AD na vzdialených lokalitách.</p> <p>Testovanie replikácií medzi jednotlivými DC.</p> <p>Testovanie vysokej dostupnosti DNS vo forme prevádzky primárneho a sekundárneho DNS servera na rôznych lokalitách.</p>		

Kontrola	súbor	1
Kontrola menšej konvencie v rámci AD. V prípade potreby vytváranie a prípadná modifikácia objektov v AD podľa schváleného postupu. Konfigurácia a kontrola monitorovania a správa NTP. Konfigurácia a kontrola komunikácie s ADFS a Exchange. Konfigurácia a kontrola group policy v zmysle platných bezpečnostných politík a procesov zákazníka. Konfigurácia a kontrola DHCP rozsahov (vrátane DNS, default gateway a ďalších parametrov). Konfigurácia a kontrola záznamov v systéme DNS. Konfigurácia a kontrola odsúhlasenej menšej konvencie v rámci DNS. Konfigurácia a kontrola nad dynamickým vytváraním záznamov v DNS v integrácií s DHCP systémom. Konfigurácia a kontrola DHCP poolu pre dynamické pridelovanie IP adries.		
Monitoring a zálohovanie	súbor	1
Konfigurácia monitorovacích agentov (SCOM, Zabbix) na jednotlivé servery, špecifikácie parametrov a ich relevantných hodnôt, ktoré je potrebné monitorovať. Definovanie požiadaviek na nastavenie monitorovacieho mechanizmu. Zaradenie zálohovania.		
Vytvorenie testovacieho prostredia	súbor	1
Vytvorenie testovacej domény minimálne z dvoch doménových radičov. Účelom testovacej domény bude odskúšanie väčších zmien pred aplikovaním na produkčnej doméne, napr. zmena alebo nasedenie novej GPO.		
Školenie a dokumentácia	súbor	1
Zaškolenie pracovníkov v rozsahu 3 človeko-dní online, alebo v priestoroch objednávateľa s nahrávaním školenia a školiaca dokumentácia.		
Systémová dokumentácia.		

3. Poskytovanie podpory

Obstarávateľ požaduje proaktívnu podporu v nasledovnom rozsahu:

a) Proaktívna podpora zahŕňa nasledovné činnosti:

- Mesačne 1 človeko-deň (na mieste – alebo vzdialene): analýza stavu logov riešenia, návrh riešenia zistených problémov, realizácia zmien a požiadaviek v nastaveniach, AD health check - profylaktika domény s písomným výstupom o náleze a navrhovaných úpravách,
- Raz ročne 1 človeko-deň (na mieste): aktualizácie, optimalizácie, upgrade, patchovanie, hĺbková kontrola stavu AD pomocou dostupných nástrojov výrobcu (napr. Microsoft Active directory Right Assesment Program – ADRAP).

b) Nadštandardná podpora

Expertná podpora nad Active Directory prostredím:

Expertné práce súvisiace s dodávkou na základe objednávky, napr. zmenové požiadavky, súvisiace s predmetom zákazky, spolupráca v prípade licenčného auditu. Poskytovanie služieb nad rámec štandardnej podpory v maximálnom rozsahu 120 Osobohodín.

Celok B): Zvýšenie bezpečnosti privilegovaných administrátorských prístupov

Predmetom zákazky v celku B) je zabezpečenie privilegovaných administrátorských prístupov.

Obstarávateľ na povýšenej doméne podľa celku A) požaduje pre potreby administrátorských činností nasadenie politiky pre rozdelenie administrátorských práv podľa štandardizovaného modelu Microsoftu (PAM - Tier model for partitioning administrative privileges).

Model vrstiev má vytvárať delenia medzi správcami na základe toho, aké zdroje spravujú. Správcovia s kontrolou nad užívateľskými pracovnými stanicami sú oddelení od tých, ktorí riadia aplikácie alebo spravujú podnikové identity. Požaduje sa uplatnenie obmedzení prihlásenia, aby sa zabezpečilo, aby vysoko privilegované účty nemali prístup k menej bezpečným zdrojom.

Pre zamestnancov IT a pre dodávateľské subjekty poskytujúce IT služby sa požaduje vytvorenie jednotlivých kategórií privilegovaných administrátorských účtov:

1. Kategória T0: - pre potreby administrátorských činností nad systémami a aplikáciami strategického významu s vysokou úrovňou dôležitosti a zabezpečenia (napr. virtuálne prostredie, Active Directory, IS zálohy a obnovy dát a pod.).
2. Kategória T1: - pre potreby administrátorských činností na serveroch spoločnosti BVS.
3. Kategória T2: - pre potreby administrátorských činností na pracovných stanicach a zariadeniach pre IT zamestnancov spoločnosti BVS.

Grafické znázornenie:

Prístupy na servery kategórie T0 a T1 majú byť cez terminálové servery, kde obstarávateľ plánuje v budúcnosti nasadenie ITM riešenia (nie je predmetom obstarávania). Počet terminálových serverov má byť štyri a majú byť logicky rozdelené podľa výstupu analýzy a požiadaviek obstarávateľa.

1. Dodávka licencií

Špecifikácia	Zoznam potrebných licencií	Počet
Licencie MS TS	Windows Server Terminal - User CAL 2022 (možnosť rozdeliť medzi 4 servermi)	100 ks

2. Inštalčné, implementačné práce a migrácia

Popis	Jednotka	Počet
Analýza	súbor	1
Analýza existujúceho stavu privilegovaných účtov. Analýza bezpečnostných GPO politík pre privilegované účty. Analýza pre rozdelenie terminálových serverov.		
Návrh riešenia	súbor	1
Návrh riešenia pre nasadenia PAM modelu pre potreby odsúhlasenia manažérom kybernetickej bezpečnosti. Návrh riešenia pre nasadenie terminálových serverov podľa určenia a podľa jednotlivých úrovní T0 a T1.		
Implementácia PAM modelu	súbor	1
Vytvorenie logického oddelenia. Zabezpečenie dostupnosti administratívnych služieb. Nakonfigurovanie príslušných povolení služieb AD. Konfiguračné úpravy serverov podľa príslušnosti k danému Tier levelu. Nasadenie GPO politík podľa PAM modelu. Inštalácia a konfigurácia štyroch terminálových serverov, ktoré budú slúžiť ako prestupné brány na systémy kategórie T0 a T1. Nakonfigurovanie administratívnych terminálových serverov.		
Testovanie	súbor	1
Testovanie funkčnosti implementovaného PAM modelu a prístupov na systémy kategórie T0 a T1 cez terminálové servery.		
Školenie a dokumentácia	súbor	1
Zaškolenie pracovníkov v rozsahu 2 človeko-dní online, alebo v priestoroch objednávateľa s nahrávaním školenia a školiaca dokumentácia. Systémová dokumentácia.		

3. Poskytovanie podpory

Obstarávateľ požaduje proaktívnu podporu v nasledovnom rozsahu:

a) Proaktívna podpora zahŕňa nasledovné činnosti:

- Mesačne 2 človeko-dni (na mieste alebo vzdialene): analýza stavu logov riešenia, návrh riešenia zistených problémov, realizácia zmien a požiadaviek v nastaveniach, dohľad nad prevádzkou, kontrola funkčnosti PAM modelu,
- Raz ročne 1 človeko-deň (na mieste): aktualizácie, optimalizácie, upgrade, patchovanie, hĺbková kontrola stavu PAM modelu a v prípade potreby vypracovanie návrhu na zlepšenie riešenia,
- Ročná aktualizácia systémovej dokumentácie.

b) Nadštandardná podpora

Expertná podpora nad PAM prostredím:

Expertné práce súvisiace s dodávkou na základe objednávky, napr. zmenové požiadavky, súvisiace s predmetom zákazky, spolupráca v prípade licenčného auditu. Poskytovanie služieb nad rámec štandardnej podpory v maximálnom rozsahu 120 osobohodín.

